Valutazione della Sicurezza Funzionale dei Sistemi Strumentali di Sicurezza

Pasquale Fanelli

Questo documento pone una mirata attenzione alle definizioni, agli obiettivi, alle annotazioni, alle specifiche considerazioni sulla Valutazione della Sicurezza Funzionale (Functional Safety Assessment) dei Sistemi Strumentali di Sicurezza (Sis) e alla Clausola di Uso Precedente, in conformità con gli Standard Internazionali EN/Iec 61508 "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems" e Iec 61511 "Functional Safety: Safety Instrumented Systems for the Process Industry Sector".

Lo Standard Iec 61511 si applica a vari settori dell'Industria di Processo, tra i quali l'Oil & Gas, la raffinazione del petrolio, il chimico, il cartario, le centrali elettriche non-nucleari. In particolare la Valutazione della Sicurezza Funzionale dei Sis fa riferimento alla clausola 8 dell'EN/Iec 61511 e alla clausola 5 dell'Iec 61511.

La Valutazione della Sicurezza Funzionale di un Sis gioca un ruolo fondamentale per poter affermare che un Sis risulti conforme ad EN/Iec 61508 e Iec 61511, laddove applicabili, durante tutto il corso delle fasi in cui si articola il Ciclo di Vita della Sicurezza (Funzionale) del Sis stesso. Ricordiamo che il Ciclo di Vita della Sicurezza (Funzionale) di un Sis tipicamente e a solo titolo di esempio, si suddivide nelle seguenti fasi: Concezione, Scopo, Analisi di Rischio, Allocazione delle funzioni di sicurezza ai Livelli di Protezione Indipendenti, Specifica dei Requisiti di Sicurezza, Progettazione e Ingegneria, Installazione, Messa in Servizio e Validazione, Esercizio e Manutenzione, Dismissione. A tali fasi vanno aggiunte la Gestione dei Test, la Gestione delle Modifiche (eventuali) e della Valutazione della Sicurezza Funzionale, di cui ci occupiamo qui di seguito in maggior dettaglio.

La "conformità" di sotto-sistemi e componenti utilizzati in Sistemi Strumentali di Sicurezza, pur in assenza di conformità allo Standard EN/Iec 61508 Parte 2, relativa ai requisiti dell'hardware e Parte 3, relativa ai requisiti del software, è resa raggiungibile nella Industria di Processo, per un livello di integrità della sicurezza fino a Sil 3, ottemperando ai requisiti della Clausola di Uso Precedente e relative sotto-clausole stabilite dallo Standard Iec 61511.

Risultano pertanto evidenti, sia la grande importanza di avere ben chiari i limiti di applicabilità degli Standard EN/Iec 61508 e Iec 61511 per poter invocare la Clausola di Uso Precedente e relative sotto-clausole, sia i vantaggi rappresentati dall'impiego nei Sis di sotto-sistemi e componenti la cui conformità ad EN/Iec 61508 Parte 2 e Parte 3, sia certificata, per applicazioni fino ai livelli di integrità della sicurezza (Sil) dichiarati, da un Ente Notificato, quale ad esempio storicamente il Tüv.

Definizione di Valutazione della Sicurezza Funzionale

La definizione di Valutazione della Sicurezza Funzionale in accordo ad Iec 61511-1 s.c. 3.2.2.6 è "Investigazione, basata su evidenza, per valutare la sicurezza funzionale raggiunta da uno o più livelli di protezione (indipendenti, ndr)". Una investigazione basata su evidenza può intendersi come una indagine a tutto campo, comprovata e suffragata da "prove" rappresentate da documentazione tipicamente di progetto, tra cui specifiche, disegni, calcoli, data base, manuali, ma anche da documentazione come manuali di sicurezza, materiale fotografico, dichiarazioni di eccezione, certificazioni e relative restrizioni di Enti Notificato, tra i quali il Tüv in particolare, *curricula* del personale impiegato nel Progetto, certificazioni interne quali Fat e Sat e altro ancora. Nelle fasi di esercizio, manutenzione e test, per la Valutazione della Sicurezza Funzionale Periodica, risulterà necessaria tutta la documentazione relativa a tali attività, così come previsto da un Sistema di Gestione della Sicurezza conforme alla normativa vigente.

Obiettivo della Valutazione della Sicurezza Funzionale

L'obiettivo della Valutazione della Sicurezza Funzionale, in accordo ad Iec 61511-1 s.c. 5.2.6.1.1, è il seguente: "Una procedura di Valutazione della Sicurezza Funzionale dovrà essere eseguita e condotta in modo da poter esprimere un giudizio sulla sicurezza funzionale e sulla integrità della sicurezza raggiunta dal Sis. La procedura dovrà richiedere che sia nominato un Team di Valutazione della Sicurezza Funzionale, che combini esperienza tecnica, applicativa e operativa richieste per la particolare installazione". Tale obiettivo dovrà essere raggiunto per poter affermare (ed eventualmente auto-certificare) che il Sis risulta pienamente conforme ad EN/Iec 61508 c. 4 e Iec 61511 c. 4, da parte di chi applica gli standard in questione. Ricordiamo che tipicamente l'EN/Iec 61508 si ap-

P. Fanelli, Functional Safety Expert e TÜV-FSEng (ID-No. 0050/04), Invensys Systems Italia SpA

plica ai Fabbricanti e Fornitori dei sotto-sistemi e dei componenti dei Sis, mentre l'Iec 61511 si applica a progettisti, agli integratori e agli utilizzatori degli stessi Sis.

Team di Valutazione della Sicurezza Funzionale

Il gruppo del Team di Valutazione della Sicurezza Funzionale, in accordo ad Iec 61511-1 s.c. 5.2.6.1.2 "dovrà includere almeno un esperto senior, non coinvolto nel Team di Progetto". Il gruppo del Team di Valutazione della Sicurezza Funzionale, dalla comprovata esperienza professionale, dovrà aver maturato una esperienza tecnica, applicativa e operativa sulla specifica applicazione. Il Responsabile e il gruppo del Team di Valutazione della Sicurezza Funzionale dovranno essere indipendenti dal Team di Progetto.

Piano di Valutazione della Sicurezza Funzionale

Un Piano di Valutazione della Sicurezza Funzionale, in accordo ad Iec 61511-1 s.c. 5.2.6.1.2, dovrà essere articolato, come segue:
1. Ambito della Valutazione della Sicurezza Funzionale;
2. Partecipanti del Team di Valutazione della Sicurezza Funzionale;
3. Capacità, Responsabilità e Autorità del Team di Valutazione della Sicurezza Funzionale;
4. Il livello di indipendenza del Team di Valutazione della Sicurezza Funzionale;
5. Identità di diversi organismi della sicurezza coinvolti nella Valutazione della Sicurezza Funzionale;
6. Le risorse necessarie per completare le attività di Valutazione della Sicurezza Funzionale;
7. Le informazioni generate dalle attività di Valutazione della Sicurezza Funzionale;
8. Piano di Rivalidazione della Valutazione della Sicurezza Funzionale, nel caso di introduzione di Modifiche.

Stadi di Valutazione della Sicurezza Funzionale

Le attività di Valutazione della Sicurezza Funzionale andranno, laddove possibile, svolte in corrispondenza dei seguenti Stadi, in concomitanza del termine di esecuzione delle corrispondenti Fasi del Ciclo di Vita della Sicurezza (Funzionale):
- Stadio 1: Fase 1 (Valutazione dei Pericoli e dei Rischi); Fase 2 (Allocazione delle Sif ai Livelli di Protezione Indipendenti e assegnazione ad ogni Sif del relativo Sil); Fase 3 (Specifica dei Requisiti di Sicurezza Srs del Sis)
- Stadio 2: Fase 4 (Progettazione e Ingegneria del Sis)
- Stadio 3: Fase 5 (Fat, Installazione, Messa in Servizio e Validazione del Sis, emissione delle Procedure di Esercizio e Manutenzione)
- Stadio 4: Fase 6 (Esercizio e Manutenzione del Sis[1]
- Stadio 5: Fase 7 (Modifica del Sis[2])

[1] Dopo aver maturato la necessaria esperienza, ma in ogni caso al termine della prima manutenzione programmata del Sis.

[2] Dopo aver effettuato eventuali modifiche di HW, SW, set, frequenza di test ecc.

Verifiche relative alla Valutazione della Sicurezza Funzionale

Prima che si presentino i pericoli identificati allo Stadio 3 di cui sopra, vale a dire prima dell'avviamento dell'Impianto, il Team di Valutazione della Sicurezza Funzionale, dovrà verificare che: a) sia stata condotta l'Analisi di Rischio; b) siano state implementate e in ogni caso risolte le raccomandazioni scaturite dalla Analisi di Rischio, riferite in particolare al Sis; c) siano in essere le Procedure di Modifica Progettuale e che siano state correttamente implementate; d) siano state implementate e in ogni caso risolte le raccomandazioni scaturite dalla Valutazione della Sicurezza Funzionale eventualmente condotta negli Stadi 1, 2; e) il Sis sia progettato, costruito e installato in accordo alla Specifica dei Requisiti di Sicurezza (Srs), e che eventuali difformità siano state identificate e risolte; f) siano in essere le Procedure Operative, le Procedure di Sicurezza, le Procedure di Emergenza, le Procedure di Manutenzione relative al Sis; g) sia appropriato il Piano di Validazione del Sis e che le attività di validazione siano state completate; h) sia stata completata la formazione del personale dell'Esercizio e della Manutenzione (e Test, in caso di funzione separata), e che le informazioni appropriate sul Sis siano state compiutamente fornite al personale; i) siano in essere un Piano implementativo della Valutazioni della Sicurezza Funzionale Periodica.

Documentazione della Valutazione della Sicurezza Funzionale

La seguente Documentazione viene tipicamente elaborata ed emessa, in relazione alla attuazione della Valutazione della Sicurezza Funzionale, in relazione agli Stadi 1, 2, 3:

Parte 1

1.1 Piano della Valutazione della Sicurezza Funzionale;
1.2 Procedure della Valutazione della Sicurezza Funzionale;
1.3 Organigramma, Qualifiche e Curricula del Team di Valutazione della Sicurezza Funzionale;
1.4 Attestazione del Grado di Indipendenza del Team di Valutazione della Sicurezza Funzionale.

Parte 2

2.1 Obiettivi e Ambito della Valutazione della Sicurezza Funzionale;
2.2 Descrizione del Sistema sottoposto alla Valutazione della Sicurezza Funzionale;
2.3 Elenco della Normativa;
2.4 Elenco dei Riferimenti;
2.5 Elenco della Documentazione di Progetto Esaminata;
2.6 Elenco delle Procedure Esaminate;
2.7 Elenco degli Strumenti di Sviluppo e Produzione Esaminati.

Parte 3

3.1 Elenco Sif e Sil allocati Adeguati e Conformi;
3.2 Elenco Sif e Sil allocati Non-adeguati e/o Non-conformi (eventuale);
3.3 Rapporto Finale della Valutazione della Sicurezza Funzionale;
3.4 Piano di Valutazione della Sicurezza Funzionale Periodica.

Documentazione della Valutazione della Sicurezza Funzionale Periodica

La seguente Documentazione viene tipicamente elaborata ed emessa, in relazione alla attuazione di una Valutazione della Sicurezza Funzionale Periodica in relazione agli Stadi 4, 5 (eventuale):

1. Rapporti della Valutazione della Sicurezza Funzionale (iniziale e successivi);
2. Rapporti delle Prove e Qualifiche del Personale preposto;
3. Rapporti di Manutenzione Ordinaria e Qualifiche dei Manutentori;
4. Rapporti di Manutenzione Straordinaria e Qualifiche dei Manutentori;
5. Rapporti di Revisione Periodica dei Fornitori e Qualifiche del personale preposto;
6. Rapporti di Modifica e relative Procedure di Approvazione;
7. Rapporti di Verifica Periodica degli Strumenti di Produzione;
8. Segnalazioni e Raccomandazioni sulla Sicurezza dell'Esercizio e/o Tecnologie.

Limiti applicativi dello Standard Iec 61511

Facendo riferimento allo Standard Iec 61511 Parte 1, nella Fig. 3 dello stesso documento si trovano chiaramente definiti i limiti applicativi sia dello Standard Iec 61511 che lo Standard EN/Iec 61508:

Hardware

Sviluppo di Nuovi Dispositivi Hardware
Segui Iec 61508

Utilizzo di Dispositivi Hardware "Provati in Uso"
Segui Iec 61511

Utilizzo di HW sviluppato e validato in accordo ad Iec 61508
Segui Iec 61511

Software

Sviluppo di SW di Sistema ("embedded")
Segui Iec 61508-3

Sviluppo di SW applicativo usando Fvl
Segui Iec 61508-3

Sviluppo di SW applicativo usando Lvl o Fpl
Segui Iec 61511

dove: Fpl sta per Fixed Program Language (solo input dati, come ad es. per trasmettitori smart); Lvl sta per Limited Variability Language (function block diagrams, ladder logic diagrams); Fvl sta per Full Variability Language (instruction list, structured text). Si fa notare che lo Standard Iec 61511 Parte 1 alla s.c. 11.5.2.2 precisa altresì che componenti e sotto-sistemi per applicazioni Sil 4 seguono unicamente lo Standard EN/Iec 61508.

[3] Il sistema di Gestione della Configurazione si può definire come il sistema di identificazione dei vari componenti soggetti ad evoluzione, quali in particolare i componenti HW e SW di un sotto-sistema, allo scopo di tenerne sotto controllo i relativi cambi, e mantenerne la continuità e la tracciabilità attraverso l'intero Ciclo di Vita del Sis.

Certificazione

La Certificazione da parte di un Ente Notificato qualificato non solo sta ad attestare la conformità allo Standard EN/Iec 61508 (Parti 1, 2, 3), ma basandosi su un complesso iter valutativo e validativo, incluse prove, ispezioni e verifiche, genera:

- Rapporti completi delle Prove e delle Ispezioni eseguite;
- Verifica validata della risposta ai guasti HW e SW;
- Uso di Sistemi di Tipo Approvato in applicazioni differenti o specifiche;
- Qualificazione delle funzioni di sicurezza attuate;
- Quantificazione dei ratei di guasto;
- Restrizioni all'Uso (recentemente incluse nel Manuale di Sicurezza del Fornitore).

La Certificazione, oltre ad attestare la conformità allo Standard EN/Iec 61508, attesta che il sotto-sistema e il componente può essere utilizzato specificatamente in un Sis fino al Livello di Integrità della Sicurezza (Sil) riportato nell'Attestato stesso e, quale aspetto più importante, dietro il vincolo delle Restrizioni all'Uso stabilite dall'Ente Notificato.
La Certificazione non affranca Progettisti, Integratori e Utilizzatori del Sis dall'ottemperare a tutti i requisiti specificati dagli Standard EN/Iec 61508 e Iec 61511, per tutte le fasi di competenza e di responsabilità previste dal Ciclo di Vita della Sicurezza (Funzionale).

Clausola di Uso Precedente

L'evidenza della idoneità di un sotto-sistema e di un componente per l'impiego in un Sis è vincolata in accordo alla Clausola di Uso Precedente dello Standard Iec 61511 e relative sotto-clausole, che vincolano a documentare e allegare al Progetto della Sicurezza Strumentale quanto segue: a) Considerazioni sul Sistema di Gestione della Qualità e sul Sistema di Gestione della Configurazione[3] del Fabbricante; b) Identificazione e specifica adeguata dei componenti e dei sotto-sistemi; c) Attestato prestazionale di componenti o sotto-sistemi in profili operativi e ambienti fisici simili; d) Esperienza operativa pregressa. Le sotto-clausole di Uso Precedente dello Standard Iec 61511 dettagliano ulteriori requisiti sulla base della tipologia dei componenti e dei sotto-sistemi e del linguaggio del software applicativo adottato. Più in particolare, per i dispositivi in campo, quali ad es. sensori, solenoidi, valvole di blocco, la sotto-clausola 11.5.3.2 dello Standard Iec 61511 stabilisce:

i) l'attestato prestazionale vale, sia per applicazioni in sistemi di sicurezza, che non;
ii) l'esperienza operativa pregressa può basarsi su un Elenco Referenze, purché: l'elenco risulti controllato e aggiornato con regolarità; l'elenco risulti esteso solo ad applicazioni dalla sufficiente esperienza operativa; l'elenco non includa i dispositivi che abbiano dimostrato di non performare; l'elenco riporti l'applicazione di processo qualora di pertinenza.

Conclusioni

Una Valutazione della Sicurezza Funzionale puntuale, efficace e periodica, eseguita da uno o più esperti indipendenti di

sicurezza funzionale, con un giudizio vincolante degli stessi di accettazione incondizionata di ogni funzione di sicurezza strumentale e di contestuale attestazione di conformità ad EN/Iec 61508 e Iec 61511, laddove applicabili, completa il quadro di un Sistema Strumentale di Sicurezza ideato, progettato, costruito, installato, validato, operato, testato, manutenuto, eventualmente modificato, in stretto accordo agli obiettivi e ai requisiti del Ciclo di Vita della Sicurezza (Funzionale), così come previsto dal Piano di Sicurezza.
Il raggiungimento e il mantenimento del livello di integrità della sicurezza funzionale del Sis risulterà in una riduzione del rischio residuo a valori inferiori a quelli del rischio tollerabile per la vita e la salute dei lavoratori, e per l'ambiente, in piena ottemperanza al principio generale dettato dall'art. 2087 c.c.: "L'imprenditore è tenuto ad adottare, nell'esercizio dell'impresa, le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro". La clausola di "Uso Precedente" dello Standard Iec 61511, penalizzante dal punto di vista della gestione della documentazione richiesta e nel contempo premiante (rif. c. 11.4.4) sotto l'aspetto della configurazione (leggi Minimum Hardware Fault Tolerance), determina a tutti gli effetti una forte assunzione di responsabilità da parte di chi decidesse per l'adozione di tali componenti, soprattutto nei caso in cui lo stesso Standard Iec 61511-1 richiede il Manuale di Sicurezza per applicazioni fino a Sil 3. La Certificazione pertanto, pur non essendo neppure citata dallo Standard Iec 61511 (tranne che per il requisito di librerie "certificate" per il software applicativo), rimane la via più decisamente percorribile per evitare, soprattutto all'atto conclusivo di una Valutazione della Sicurezza Funzionale decisamente critica come quella di Stadio 3 (vedi sopra), la temibile "sorpresa" della non conformità. In una catena di sicurezza è l'anello più debole l'elemento determinante la debolezza dell'intera catena, sia dal punto di vista delle prestazioni, che della Conformità.

Riferimenti

[1] "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems", *EN/Iec 61508*.
[2] "Functional Safety: Safety Instrumented Systems for the Process Industry Sector" , *Iec 61511*, 2003.
[3] P. Fanelli, "Profilo Applicativo degli Standard Iec 61508 e Iec 61511"; *Seminario sulla Sicurezza Funzionale*, 2004
[4] P. Fanelli, "Assegnazione degli Obiettivi Prestazionali di un Sistema di Sicurezza Strumentale in accordo allo Standard EN/Iec 61508", *Seminario sulla Sicurezza Funzionale*.